

REMARKS

In the non-final Office Action dated October 19, 2007 (paper no. 20071010), the Examiner objected to claim 1; rejected claims 1-4, 6-10, 31-32, 35, 37-40, 50-51, 82-83, and 86-87 under 35 U.S.C. § 102(b) over U.S. Patent No. 5,577,209 to Boyle et al. ("Boyle"); and rejected claims 5, 33-34, 36, and 84-85 under 35 U.S.C. § 103(a) over Boyle and U.S. Patent No. 5,991,877 to Luckenbaugh ("Luckenbaugh").

Claims 1-10, 31-40, 50-51, and 82-87 are pending in this application. For the reasons discussed in detail below, applicants submit that the pending claims are in condition for allowance.

A. Applicants' Technology

Applicants' technology is directed to remotely managing multiple network security devices using a security manager device and intermediate supervisor devices. Applicants' security manager device distributes security control information – such as a security policy template – to intermediate supervisor devices, each of which may be a primary supervisor device for multiple network security devices. In turn, each intermediate supervisor device distributes the security control information to each of the multiple network security devices for which it is the primary supervisor device. Once the security policy template has been received by a network security device, it may be configured with information that is specific to the network security device.

As each network security device executes the security control information or security policy, it gathers network security information related to its activities and the network information it monitors. If its primary supervisor device is available, the network security device sends this gathered network security information to the primary supervisor device, which stores and processes the information. On the other hand, if the primary supervisor device is unavailable, the network security device instead sends its gathered network security information to an alternate supervisor device, which stores and processes

the information. The security manager retrieves the network security information from each of the intermediate supervisor devices that store a portion of the information and aggregates the retrieved information. The aggregated network security information may be used to determine whether a security policy is correctly implemented, identify security concerns, and produce reports about network information.

B. Boyle

Boyle describes a system for providing security for a non-secure network, such as a network in which neither network assets nor hosts are trusted. Rather than replace existing network assets and hosts with trusted network assets and hosts, Boyle implements secure network interface units (SNIUs) between each host or user computer and the network. Boyle describes a security manager that controls the operation and configuration of multiple SNIUs. The functions of the security manager may be distributed over three platforms – an SNIU security manager (SSM), an area security manager (ASM), and a network security manager (NSM). Implementing an SNIU at each computer on a network effectively establishes a security perimeter for the network.

C. Claim Objections

The Examiner objected to claim 1. Applicants have amended claim 1 to address the Examiner's objections. In particular, this claim has been amended to recite "so that the security manager device can efficiently distribute security control information to multiple network security devices." Accordingly, applicants respectfully request that the objection to claim 1 be withdrawn.

D. Prior Art Rejections

The Examiner has rejected claims 1-10, 31-40, 50-51, and 82-87 over Boyle, alone under 35 U.S.C. § 102(b) or in combination with another reference under 35 U.S.C.

§ 103(a). For the reasons discussed below, applicants respectfully traverse these rejections.

Claims 1-10 recite "distributing security control information to multiple network security devices, the security control information to be used to generate network security information" and "the network security information generated by an indicated one of the multiple network security devices using the security control information." That is, a network security device uses security control information – such as a security policy – that has been distributed to the network security device to generate network security information – such as information related to the network security device's activities and the network information it monitors. Boyle does not disclose or suggest "distributing security control information to multiple network security devices, the security control information to be used to generate network security information" and "the network security information generated by an indicated one of the multiple network security devices using the security control information." The Examiner cites Boyle at 3:30-42 and 8:50-66 as corresponding to these recited features. (Office Action, Oct. 19, 2007, p. 3-4.) Boyle at 3:30-42 describes that its Security Manager distributes network security functions over three platforms – its SSA, ASM, and NSM – and describes several of the security functions performed by each platform with regard to an SNIU or group of SNIUs. The Examiner apparently believes that Boyle's "SNIUs" correspond to applicants' "network security devices." However, nowhere does the cited portion of Boyle indicate that an SNIU receives information that corresponds to applicants' "security control information" which is used by the SNIU to generate information that corresponds to applicants' "network security information."

Nor does Boyle at 8:50-66 disclose or suggest "distributing security control information to multiple network security devices, the security control information to be used to generate network security information" and "the network security information generated by an indicated one of the multiple network security devices using the security control information." This cited portion describes the initialization of Boyle's security system, including the SNIUs. However, nowhere does this cited portion indicate that an SNIU

receives information that corresponds to applicants' "security control information" which is used by the SNIU to generate information that corresponds to applicants' "network security information." Boyle does not disclose or suggest "distributing security control information to multiple network security devices, the security control information to be used to generate network security information" and "the network security information generated by an indicated one of the multiple network security devices using the security control information."

Claims 1-10 also recite "determining a supervisor device that is the primary supervisor device for each of the multiple network security devices." Claims 31-40, 50-51, and 82-87 recite "the security devices with which the supervisor device is associated." That is, each primary supervisor device is associated with multiple network security devices. Boyle does not disclose or suggest "determining a supervisor device that is the primary supervisor device for each of the multiple network security devices" or "the security devices with which the supervisor device is associated." The Examiner cites Boyle at 3:30-42 as corresponding to this recited feature. In particular, the Examiner cites Boyle's "Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to its [sic] assigned SNIUs." (Office Action, Oct. 19, 2007, p. 3.) The Examiner apparently believes that Boyle's "SSA" corresponds to applicants' "primary supervisor device," and that Boyle's "SNIUs" correspond to applicants' "network security devices." However, the portion of Boyle cited by the Examiner makes clear that each of Boyle's SSAs is assigned to only one SNIU, rather than multiple SNIUs as in applicants' techniques. This cited portion describes, "The SSA exchanges data and commands with its assigned SNIU, and performs [services] for the SNIU" (emphasis added). Boyle's Figure 5A confirms that each SSA is assigned to one SNIU, illustrating that each SNIU includes a single SSA. Thus, unlike applicants' techniques, each of Boyle's SSAs is not associated with multiple SNIUs. Boyle does not disclose or suggest "determining a supervisor device that is the primary supervisor device

for each of the multiple network security devices" or "the security devices with which the supervisor device is associated."

Claims 1-10 also recite "sending a single copy of the security control information to the determined supervisor device" and "indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices." That is, the same security control information that is sent to the supervisor device is sent to each of the network security devices associated with the supervisor device. Boyle does not disclose or suggest "sending a single copy of the security control information to the determined supervisor device" and "indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices." The Examiner cites Boyle at 3:30-42 and 8:50-66 as corresponding to these recited features. In particular the Examiner believes that Boyle's "Security Manager (SM) which distributes security functions to SSA (SNIU security agent) and SSA in return distributes the security functions to its [sic] assigned SNIUs" so corresponds. While Boyle at 3:30-42 describes that its Security Manager distributes network security functions to its SSA, ASM, and NSM, nowhere does it indicate that these network security functions are distributed by the SSA to an SNIU. At most, this cited portion indicates that "[t]he SSA exchanges data and commands with its assigned SNIU, and performs [services] for the SNIU."

Nor does Boyle at 8:50-66 disclose or suggest "sending a single copy of the security control information to the determined supervisor device" and "indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices." This cited portion describes the initialization of the security system, including the SNIUs. However, nowhere does this cited portion indicate that the security functions that were distributed to the SSA are in turn distributed by the SSA to the SNIUs. Boyle does not disclose or suggest "sending a single copy of the security control information to the determined supervisor device" and "indicating to the determined

supervisor device to send a copy of the security control information to each of the multiple network security devices."

Claims 31-49 and 82-87 recite "distributing the security policy implementation information to each of the determined supervisor devices" and "indicating to each of the determined supervisor devices to distribute the security policy implementation information to the security devices with which the supervisor device is associated." Claims 50-51 recite "distributing the control information to each of the determined supervisor devices" and "indicating to each of the determined supervisor devices to distribute the control information to the security devices with which the supervisor device is associated." That is, the same security policy implementation (or control) information that is sent to the supervisor devices is sent to each of the network security devices associated with the supervisor devices. Boyle does not disclose or suggest these recited features any more than it discloses or suggests "sending a single copy of the security control information to the determined supervisor device" and "indicating to the determined supervisor device to send a copy of the security control information to each of the multiple network security devices" as recited in claims 1-10. The Examiner again cites Boyle at 3:30-42 as corresponding to these recited features. (Office Action, Oct. 19, 2007, p. 8-9, 11.) For at least the reasons discussed above in reference to claims 1-10, Boyle does not disclose or suggest "distributing the security policy implementation [or control] information to each of the determined supervisor devices" and "indicating to each of the determined supervisor devices to distribute the security policy implementation [or control] information to the security devices with which the supervisor device is associated."

Claims 1-10 further recite "notifying the primary supervisor device for the indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices." That is, the security manager notifies the primary supervisor device of all of the supervisor devices that have stored network security information generated by a network security device. Boyle does not disclose or suggest "notifying the primary supervisor device for the

indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices." The Examiner cites Boyle at 9:5-15 as corresponding to this recited feature. In particular, the Examiner believes that Boyle's "negotiates SNIU pairings with all other ASMs" so corresponds. (Office Action, Oct. 19, 2007, p. 4.) Boyle at 9:5-15 describes that when an ASM fails, the network can automatically switch over to an alternate ASM. When a failed ASM is re-initialized, it may negotiate SNIU pairings with the other ASMs in operation. The described negotiation, or communication, is between an ASM and an ASM. The Examiner's position is inconsistent. As described above, the Examiner previously indicated that it is Boyle's "Security Manager" that corresponds to applicants' security manager device, and that it is Boyle's "SSA" that corresponds to applicants' primary supervisor device. The Examiner cannot now indicate that one of Boyle's "ASMs" corresponds to applicants' security manager device, and that another one of Boyle's "ASMs" corresponds to applicants' primary supervisor device. Boyle does not disclose or suggest "notifying the primary supervisor device for the indicated network security device of a desire for the generated network security information, the notifying including an indication of the determined alternate supervisor devices."

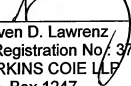
E. Conclusion

In view of the above amendment, applicants believe the pending application is in condition for allowance and respectfully request a prompt notice of allowance.

Please charge any deficiency in fees or credit any overpayment to our Deposit Account No. 50-0665, under Order No. 248588002US1 from which the undersigned is authorized to draw.

Dated: 4/14/08

Respectfully submitted,

By 
Steven D. Lawrenz
Registration No.: 37,376
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8000
(206) 359-7198 (Fax)
Attorney for Applicant